United States General Accounting Office

GAO

Report to Congressional Requesters

May 2004

DEFENSE ACQUISITIONS

Knowledge of Software Suppliers Needed to Manage Risks

GAO-04-678

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Acquisitions. Knowledge of Software Suppliers Needed to Manage Risks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
http://www.gao.gov/new.items/d04678.pdf

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**33**	

May 2004

DEFENSE ACQUISITIONS

Knowledge of Software Suppliers Needed to Manage Risks

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-678, a report to congressional requesters

Why GAO Did This Study

The Department of Defense (DOD) is increasingly reliant on software and information systems for its weapon capabilities, and DOD prime contractors are subcontracting more of their software development. The increased reliance on software and a greater number of suppliers results in more opportunities to exploit vulnerabilities in defense software. In addition, DOD has reported that countries hostile to the United States are focusing resources on information warfare strategies. Therefore, software security, including the need for protection of software code from malicious activity, is an area of concern for many DOD programs.

GAO was asked to examine DOD's efforts to (1) identify software development suppliers and (2) manage risks related to foreign involvement in software development on weapon systems.

What GAO Recommends

To address software vulnerabilities and threats, GAO recommends that DOD better define software security requirements and require program managers to mitigate associated risks accordingly.

DOD agreed with the findings but only partially concurred with the recommendations over concerns that they place too much responsibility for risk mitigation with program managers. GAO has broadened the recommendations to address DOD's concerns.

www.gao.gov/cgi-bin/getrpt?GAO-04-678.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Katherine Schinasi at (202) 512-4841 or schinasik@gao.gov.

What GAO Found

DOD acquisition and software security policies do not fully address the risk of using foreign suppliers to develop weapon system software. The current acquisition guidance allows program officials discretion in managing foreign involvement in software development, without requiring them to identify and mitigate such risks. Moreover, other policies intended to mitigate information system vulnerabilities focus mostly on operational software security threats, such as external hacking and unauthorized access to information systems, but not on insider threats, such as the insertion of malicious code by software developers. Recent DOD initiatives may provide greater focus on these risks, but to date have not been adopted as practice within DOD.

While DOD has begun to recognize potential risks from foreign software content, this is not always the case within the weapon programs where software is developed or acquired. Program officials for the systems in this review did not make foreign involvement in software development a specific element of their risk identification and mitigation efforts. As a result, program officials' knowledge of the foreign developed software included in their weapon systems varied. In addition, risk mitigation efforts emphasized program level risks, such as meeting program cost and schedule goals, instead of software security risks. Further, program officials often delegated risk mitigation and source selection to contractors who are primarily concerned with software functionality and quality assurance, rather than specifically addressing software security for development risks associated with foreign suppliers. Unless program officials provide specific guidance, contractors may favor business considerations over potential software development security risks associated with using foreign suppliers.

As the amount of software on weapon systems increases, it becomes more difficult and costly to test every line of code. Further, DOD cannot afford to monitor all worldwide software development facilities or provide clearances for all potential software developers. Therefore, the program manager must know more about who is developing software and where early in the software acquisition process, so that it can be included as part of software source selection and risk mitigation decisions.

Contents

Letter 1

Results in Brief 2
Background 4
DOD's Approach to Software Security Does Not Fully Address Risks from Foreign Suppliers 6
Program Officials Generally Did Not Manage Risks from Foreign-Developed Software 11
Conclusions 18
Recommendations for Executive Action 19
Agency Comments and Our Evaluation 19

Appendix I **Scope and Methodology** 22

Appendix II **Comments from the Department of Defense** 24

Appendix III **Staff Acknowledgments** 29

Abbreviations

COTS	commercial-off-the-shelf
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DSS	Defense Security Service
ITAR	International Traffic in Arms Regulations
SEI	Software Engineering Institute

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 25, 2004

The Honorable Christopher Shays
Chairman, Subcommittee on National Security,
Emerging Threats and International Relations
Committee on Government Reform
House of Representatives

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information
Policy, Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

The Department of Defense (DOD) is experiencing significant and increasing reliance on software and information systems for its weapon capabilities, while at the same time traditional DOD prime contractors are subcontracting more of their software development to lower tier and sometimes nontraditional defense suppliers. Because of economic incentives and business relationships, these suppliers are using offshore locations and foreign companies to complete various software development and support tasks. DOD is also using more commercial-off-the-shelf (COTS) software[1] to reduce development costs and allow for frequent technology updates, which further increases the number of software developers with either direct or indirect access to weapon system software. The increased dependence on software capability, combined with an exposure to a greater variety of suppliers, results in more opportunities to exploit vulnerabilities in defense software. Software security, including the protection of software code from hacking and other malicious tampering, is therefore an area of concern for many DOD systems.

[1] COTS software is that which is not specifically developed for military use and instead purchased "as-is" from an outside vendor.

As DOD's need for software increases, knowledge about foreign suppliers[2] in software development is critical for identifying and mitigating risks. Multiple national security policies and other guidance recognize the inherent risks associated with foreign access to sensitive information and technology. For 2001, the Defense Security Service (DSS) reported a significant increase in suspicious attempts by foreign entities to access U.S. technology and information, with one-third of that activity coming from foreign government-sponsored or affiliated entities. While both U. S.- and foreign-developed software are vulnerable to malicious tampering, DSS specifically noted a concern with the potential exploitation of software developed in foreign research facilities and software companies located outside the United States working on commercial projects related to classified or sensitive programs. As foreign companies and individuals play a more significant role in software development activities, the need for knowledge to manage associated risks also increases. At your request, we (1) examined DOD's efforts to identify and address risks associated with foreign involvement in software development in weapon systems and (2) determined how weapon system program offices manage these risks in individual programs.

To perform our work, we collected information from various DOD officials and software development experts and reviewed relevant guidance and procedures for software development security. We identified 16 DOD weapon systems of varying age and software capability and solicited information from system program offices and prime contractors. Complete details of our scope and methodology are located in appendix I. We performed our work from April 2003 to May 2004 in accordance with generally accepted government auditing standards.

Results in Brief

DOD acquisition and software security policies do not require program managers to identify and manage the risks of using foreign suppliers to develop weapon system software. The primary focus of the acquisition policies is to acquire weapon systems to improve military capability in a timely and cost-effective manner. Despite the inherent risks associated with foreign access to sensitive information and technology, the guidance allows program officials discretion in managing risks related to foreign

[2] For the purposes of this report, a foreign supplier is defined as any foreign company or foreign national working for companies either in the United States or abroad. It encompasses both prime contractors and subcontractors performing work under those contracts.

involvement in software development. Other requirements and policies intended to mitigate information system vulnerabilities focus primarily on operational software security threats, such as external hacking and unauthorized access to information systems, but not on insider threats such as the insertion of malicious code by software developers. While recent DOD initiatives, such as the establishment of working groups to evaluate software products and security processes, may help to increase DOD's focus on software security and may lead to the development and identification of several potential software security best practices, they have yet to be implemented in weapon acquisition programs.

Given broad discretion, program officials for 11 of the 16 software intensive weapon systems we reviewed did not make foreign involvement in software development a specific element of their risk management efforts. As a result, the program offices had varying levels of awareness of the extent of software developed by foreign suppliers on their systems. Program officials generally did not consider the risks associated with foreign suppliers substantial enough to justify specific attention, and instead focused their resources on meeting software development cost and schedule goals while ensuring software functionality and quality. In addition, most of the program offices relied on their defense contractors to select software subcontractors and ensure that best available software development practices were being used, such as peer review and software testing. Without specific guidance from program officials, contractors primarily focused their software development efforts on meeting stated performance requirements, such as software quality and functionality, rather than mitigating potential software development security risks associated with using foreign suppliers. Contractors that excluded foreign suppliers from their programs' software development did so to avoid the additional costs and resources needed to mitigate the risks of using such suppliers.

As the amount of software on weapon systems increases, it becomes more difficult and costly to test every line of code, and DOD cannot afford to monitor all worldwide software development facilities or provide clearances for all potential software developers. Program managers who know more about potential software development suppliers early in the software acquisition process will be better equipped to include software security as part of source selection and risk mitigation decisions. Therefore, we are making three recommendations to the Secretary of Defense to ensure such knowledge is available to address risks attributable to software vulnerabilities and threats. In written comments on a draft of this report, DOD agreed with our findings that malicious code

is a threat that is not adequately addressed in current acquisition policies and security procedures and stated that the department is working to strengthen software related risk management activities. However, DOD only partially agreed with our recommendations over concerns that responsibility for mitigating risks would be placed on program managers and software assurance experts alone. We made adjustments to our recommendations to acknowledge the value of having other DOD organizations involved in software security risk management.

Background

To protect the security of the United States, DOD relies on a complex array of computer-dependent and mutually supportive organizational components, including the military services and defense agencies. It also relies on a broad array of computer systems, including weapon systems, command and control systems, financial systems, personnel systems, payment systems, and others. These systems are, in turn, connected with other systems operated by contractors, other government agencies, and international organizations. In addition, performance requirements for weapon systems have become increasingly demanding, and breakthroughs in software capability have led to a greater reliance on software to provide more weapon capability when hardware limitations are reached. As such, DOD weapon systems are subject to many risks that arise from exploitable software vulnerabilities. Software code that is poorly developed or purposely injected with malicious code could be used to disrupt these and other DOD information systems, and potentially others connected to the DOD systems.

DOD has reported that countries hostile to the United States are focusing resources on developing information warfare strategies. For example, a DSS report noted that in 2001 there was a significant increase in suspicious attempts by foreign entities to access U.S. technology and information and that trend is expected to continue. Information systems technology was the most sought after militarily critical technology by these entities. Forty-four countries were associated with attempts at accessing U.S. information technology, with 33 percent of the activity coming from foreign government-sponsored or affiliated entities. Because the U.S. defense industry is at the forefront of advanced design and development of weapon systems that include militarily critical technologies, access is sought after for industrial and financial purposes. Access to these technologies by potential adversaries could enhance the performance of their military systems and may be used to counter U.S. capabilities. DSS specifically noted a concern with exploitation or insertion of malicious code with the use of foreign research facilities and software development companies located outside the United States

working on commercial projects related to classified or sensitive programs.

Multiple requirements and guidance are in place to ensure the protection of U.S. national security interests. They generally acknowledge the inherent risk associated with foreign access to classified and export-controlled information and technology by establishing procedures to manage such access. For example, the National Industrial Security Program Operation Manual[3] establishes mandatory procedures for the safeguarding of classified information that is released to U.S. government contractors. It generally limits access to U.S. citizens with appropriate security clearances and establishes eligibility policies for U.S. contractors determined to have foreign ownership, control, or influence. Further, an additional DOD directive requires programs containing classified military information to have controls to prevent the unauthorized release of this information to foreign recipients.[4] In addition, the International Traffic in Arms Regulations (ITAR) controls foreign access to defense articles and services through the establishment of the export license and authorization process. U.S. entities, including defense contractors, may apply to the Department of State for authorization to export controlled information and technology to qualified foreign recipients, which is determined through the approval or denial of license requests.

DOD estimates that it spends about 40 percent of its Research, Development, Test, and Evaluation budget on software—$21 billion for fiscal year 2003. Furthermore, DOD and industry experience indicates that about $8 billion of that amount may be spent on reworking software because of quality-related issues. Carnegie Mellon University's Software Engineering Institute (SEI), recognized for its expertise in developing best practices for software processes, has developed models and methods that define and determine organizations' software process maturity. Better software development practices are seen as a way to reduce the number of software defects and therefore improve overall software quality, but alone the practices cannot be expected to address malicious software development activities intended to breach security. To underscore the

[3] The National Industrial Security Program Operating Manual, DOD 5220.22-M, prescribes specific requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information to U.S. contractors.

[4] DOD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992.

importance of securing software-related products, the Office of the Assistant Secretary of Defense (Networks and Information Integration) and the Federal Aviation Administration Chief Information Office are co-sponsoring, with the involvement of the Department of Energy, the National Aeronautics and Space Administration, and SEI, a project aimed at developing ways to provide safety and security assurance extensions to integrated software maturity models.

DOD's Approach to Software Security Does Not Fully Address Risks from Foreign Suppliers

DOD's approach to software development and acquisition generally focuses on improving overall quality, leaving decision making on software suppliers and security with individual program managers. Despite the risks associated with foreign access to defense systems, DOD acquisition policy does not require program managers to identify and manage the amount of foreign involvement for software development in weapon systems. DOD information system security requirements focus on operational software threats, rather than potential threats posed by software developers. While recent DOD initiatives could increase DOD's focus on software security, efforts to date have not translated into greater knowledge for program managers about foreign software development activities.

DOD Acquisition Policy Allows Discretion in Managing Foreign Software Suppliers

DOD acquisition policy[5] allows program managers discretion in managing foreign suppliers used for software development. This policy consists of general guidance for meeting overall acquisition management principles and instructs program managers to use systems engineering practices, when applicable, that focus on cost, schedule, and performance of the system. For software acquisition, program managers are encouraged to develop open software systems architectures, use COTS computer system products, and allow incremental improvements based on reusable software. All of these practices, while having the potential to benefit cost and schedule for weapon programs, could result in greater software vulnerabilities by introducing potentially malicious code from unknown software development sources. While DOD acquisition policy requires major weapon programs to maintain information about the software project's size, effort, schedule, and quality to track the cost-related implications of software development, it does not require program

[5] The DOD 5000 series includes the mandatory DOD Directive 5000.1 "The Defense Acquisition System," DOD Instruction 5000.2 "Operation of the Defense Acquisition System," and a nonmandatory Interim Defense Acquisition Guidebook.

managers to identify and manage suppliers or the potential security risks from foreign suppliers.

On October 30, 2002, DOD issued the Interim Defense Acquisition Guidebook, which contained the following security considerations to be used when foreign nationals participate in software development.

- The change control process[6] shall indicate whether foreign nationals, in any way, participated in software development, modification, or remediation.
- Foreign nationals employed by contractors or subcontractors to develop, modify, or remediate software code specifically for DOD shall each have a security clearance commensurate with the level of the program in which the software is being used.
- Primary vendors on DOD contracts may have subcontractors who employ cleared foreign nationals that work only in a certified or accredited environment.
- DOD software with coding done in foreign environments or by foreign nationals shall be reviewed by software quality assurance personnel for malicious code.
- Vendors of COTS software that demonstrate efforts to minimize the security risks associated with foreign nationals that have developed, modified, or remediated the COTS software being offered shall be given preference during the contracting process in product selection or evaluation.
- Software quality assurance personnel shall check software sent to locations not directly controlled by DOD or its contractors for malicious code when returned to the DOD contractors' facilities.

While this guidance acknowledges the additional risks from using foreign nationals in software development, it is not mandatory and, according to the Guidebook, is to be used at the discretion of acquisition program managers as best practices or lessons learned. Even if the suggested guidance was implemented, the procedures for addressing software security are generally for use after software suppliers have been selected,

[6] This process tracks changes and documents updates to a software baseline.

and do not provide the program manager the opportunity to evaluate whether the risks associated with using those suppliers for software development are acceptable. Further, several of these procedures would not apply when contractors use foreign nationals to develop unclassified portions of software programs. In support of DOD guidance, Air Force, Army, and Navy regulations implement DOD-wide acquisition policies. As such, they defer to DOD guidance and do not specifically address software security issues and related risks that may be inherent with foreign software development.

Information Assurance Focuses on Mitigating Operational Software Security Risks, Leaving Internal Software Development Vulnerable

Laws, requirements, and policies that are intended to provide information assurance for operational security do not fully address risks during software development. Under the Federal Information Security Management Act of 2002, all executive agencies, including DOD, are required to ensure that information security policies, procedures, and practices are adequate.[7] In this regard, DOD is required to carry out an information assurance program that includes the development of essential information assurances technologies and programs.[8] Generally, this includes a review of security features and information technology system safeguards. For example, DOD's information assurance policy establishes procedures to maintain the integrity of DOD information systems.[9] It sets out a process for all DOD information systems to achieve, among other things, an appropriate level of confidentiality, integrity, knowledge of threats and vulnerabilities, trustworthiness of users and interconnecting systems, and cost effectiveness. These procedures are intended to mitigate system vulnerabilities from operational threats, such as external hacking and unauthorized access to information systems. However, they do not apply to internal threats that could affect the integrity of the software, such as the insertion of malicious code during software development. In implementing its information assurance policy, DOD also relies on other

[7] Federal Information Security Management Act, Title III, E-Government Act of 2002, P.L. 107-347, Dec. 17, 2002.

[8] Enacted in the National Defense Authorization Act for Fiscal Year 2000, P.L. 106-65, Oct. 5, 1999, subsequently amended in various statutes, and currently at 10 U.S.C. § 2224.

[9] Information assurance is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation, which includes software certification for functionality and quality. DOD Directive 8500.1, "Information Assurance", Encl. 2, § E2.1.17 (Oct. 24, 2002). DOD's Information Assurance policy is implemented in DOD Instruction 8500.2, "Information Assurance Implementation" (Feb. 6, 2003).

governmentwide policies and standards. For example, DOD requires the evaluation and validation of information assurance software products, such as firewalls and intrusion detection systems, in accordance with National Security Telecommunications and Information Systems Security Policy No. 11.[10] This policy requires the use of one of three nationally recognized evaluation and validation standards.[11] However, these policies and standards do not include criteria to specifically identify and manage the use of foreign software suppliers.

To assist systems in meeting information assurance requirements, DOD has developed the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) as a standardized evaluation process.[12] This process includes a review by a designated approving official who certifies that the security features and information technology system safeguards will maintain information assurance through the life cycle of a system. The process results in an agreement between the program manager, the intended user of the system being certified, and the approval authorities that defines critical schedule, budget, security, functionality, and performance issues. The process includes a requirement for a threat assessment, but does not articulate how this information should be developed or reported. As such, it does not direct program managers to consider foreign involvement in software development as a risk or threat that needs to be addressed for information system security. In addition, while the process is mandatory, the implementation details may be tailored and, in some cases, integrated with other acquisition activities and documentation. According to DOD Software Assurance Program officials, the DITSCAP approving authority is not expected to evaluate whether the risks have been identified appropriately, only that the process will mitigate the risks identified. If the program manager has

[10] The National Security Telecommunications and Information Systems Security Policy No. 11 is a national policy to ensure that COTS information assurance and information assurance-enabled products that provide security services as an associated feature and are purchased by the U.S. government to be used in national security systems perform as prescribed by the software developer. The policy requires use of preapproved products to meet information assurance needs.

[11] The standards are the (1) Common Criteria for Information Security Technology Evaluation, (2) the National Security Agency/National Institute of Standards and Technology National Information Assurance Partnership Evaluation and Validation Program, and (3) the National Institute of Standards and Technology Federal Information Processing Standard Validation Program.

[12] DOD Instruction 5200.40 (Dec. 30, 1997).

not identified risks from foreign suppliers, the process cannot be expected to mitigate them.

DOD also requires weapon programs to protect certain types of information during transfer of technology to foreign entities. For example, documents such as the Technology Assessment/Control Plan and the Program Protection Plan address the risks associated with the potential release of information to foreign governments through cooperative programs and foreign military sales, but the documents do not provide information on specific suppliers who will be performing work, such as software developers. The Technology Assessment/Control Plan establishes planning requirements for the potential release of sensitive information to foreign entities involved in cooperative programs or purchasing military equipment. It evaluates the risk of releasing critical military capability or sensitive information and technology against the benefit of the sale to the United States. The plan also outlines the security requirements to prevent compromise. The purpose of the Program Protection Plan is to identify measures to protect Critical Program Information[13] from hostile collection efforts and unauthorized disclosure during the acquisition process.

Initiatives to Address Software Concerns Have Yet to be Implemented

While DOD has taken steps to strengthen software acquisition practices, it has yet to implement practices to better manage software development security risks in weapon programs. Currently, each of the military services is developing plans for improving software acquisition. The improvement plans are each at varying stages of development and include practices such as pilot programs for providing information on software metrics, additional training programs, and teaming arrangements with SEI for improved overall software management. DOD has also begun policy-level initiatives focused on better software management and on identifying and specifying software security processes and technologies to protect systems and network capabilities from various internal and external threats. Specific initiatives include the following:

- The Tri-Service Assessment Initiative began in 1999 to strengthen software acquisition and development as well as address repeated

[13] Critical Program Information is defined as program information, technologies, or systems that, if compromised, would degrade combat effectiveness, shorten the expected combat effective life of the system, or significantly alter program direction. This includes classified military information or unclassified controlled information about such critical programs, technologies, or systems.

performance shortfalls attributed to software. Task forces conducted detailed assessments of software-intensive programs to identity potential improvements in overall software acquisition processes.

- A source selection criteria working group is tasked with clarifying the policy on source selection criteria for software intensive systems and the application of software product maturity measures. Another working group is tasked with developing a proposal for a centralized clearinghouse of software best practices, but DOD has not approved any proposals.

- In October 2003, the Office of the Assistant Secretary of Defense (Networks and Information Integration) established the position of Deputy Director for Software Assurance that is, as part of its function, to coordinate software security efforts with other existing initiatives concerning software protection, antitamper technologies, and software producibility. In addition, since its inception, the office has initiated working groups intended to focus on mitigating software risks and improving software security. To date, while these initiatives have presented top level findings and recommendations within DOD and in public forums, they have not externally published reports or obtained funding for implementing the recommendations.

While these plans and initiatives may help to increase DOD's focus on software security and may lead to the development and identification of several potential software security best practices, DOD software assurance officials acknowledge that significant effort remains to adequately mitigate software risks to weapon systems.

Program Officials Generally Did Not Manage Risks from Foreign-Developed Software

While DOD initiatives have begun to recognize potential risks from foreign software suppliers, this is not always the case within the weapon programs where software is developed or acquired. Program officials for most of the systems we reviewed did not make foreign involvement in software development a specific element of their risk identification and mitigation efforts. As a result, program officials' knowledge of the foreign-developed software included in their weapon systems varied. In addition, risk mitigation efforts emphasized program level risks, such as meeting program cost and schedule goals, instead of software security risks. Further, program managers often delegated risk mitigation and source selection to their prime contractors who tended to be concerned with software functionality and quality assurance, rather than specifically addressing software development risks associated with foreign suppliers.

Program Office Knowledge of Software Suppliers Varied Across Weapon Systems

Knowledge of the extent of foreign involvement in software development varied greatly for the 16 weapon system programs we reviewed. Overall, the knowledge program managers had was based on the function of the software being developed, the manner in which it was acquired, and the specific handling requirements. While none of these programs could fully identify all foreign-developed software for their systems, six program offices had significant knowledge of foreign software developers.

Knowledge of software developed for weapon systems can vary based on the different functions needed to meet mission requirements. Program offices were most knowledgeable about the foreign-developed software for the onboard portions of their programs, with 4 program offices able to identify all the software produced by foreign suppliers, and 11 program offices able to identify at least some of the software produced by foreign suppliers. Onboard software is that which actually runs the weapon system, even if that software is not located on the main component (aircraft, missile, satellite, etc). For example, onboard software for a missile system could include software located on a remote platform used to guide the missile toward its target. Because onboard software is the most critical for meeting mission requirements and other program goals, program managers placed greater emphasis on the quality, functionality, and usually, the security of this software. In 9 of the systems we reviewed, either prime contractors or major subcontractors conducted software development for the onboard systems. However, in meeting with prime contractors, we found that while this increased their knowledge about foreign software suppliers, the information was not always shared with government program managers, and therefore was not available for them to use to make risk management decisions to address software security.

Program offices and contractors reported very little knowledge about the level of foreign involvement for offboard software. This software, sometimes referred to as ground based, interacts with the onboard system to provide updated information in support of operational activity. For example, one program uses standard mission planning software that interacts with the onboard flight software to provide information used for navigation and targeting. In addition, offboard software is often used to check for errors or malicious code and to produce, maintain, or verify onboard software. Program officials from 10 of the programs we reviewed indicated they had very little knowledge of the developers for their offboard software, including those portions that may have been developed by foreign suppliers.

As DOD is attempting to find new ways of reducing the time and money it takes to develop software code, the increased use of COTS software may introduce additional risks and further limit visibility into the existence of foreign-developed software. Officials for 13 of the programs reviewed had almost no insight into the use of foreign developers for any COTS software placed on their systems. Even when procured directly from a known supplier, program officials could not guarantee whether additional subcontractors were used for software development. According to DOD and program officials, visibility into COTS software is limited by the willingness of the producers of that software to share information on how the code was developed. For one program we reviewed, a substantial portion of the system was a commercial acquisition. As such, the software product was not originally developed for DOD and therefore the program office had no knowledge of software development suppliers because it did not purchase the rights to the software. Further, officials from five programs told us that the cost of identifying and managing foreign software suppliers, especially for COTS software, could be substantial. Officials from two programs said that even if available, this information would not offer significant software security improvements in light of the cost required for identifying foreign suppliers of COTS software. DOD and program officials have indicated that commercial software producers often demand a cost premium to share software and source code information that would be required to determine this information.

Similar to COTS, software from other applications and embedded software is often accepted without full knowledge of the source of development. Legacy, or reused code, is most prevalent when software programs are updated into newer versions or when software just requires editing and enhancing the older code rather than developing new code. When asked to produce software similar to what they have developed previously, manufacturers can use all or part of the legacy code as a basis for developing or modifying the new code. Ten of the programs reviewed accepted legacy software without fully identifying the sources of development. Software is also developed as part of the hardware components it is tasked with managing. This embedded software is used to control other electronic hardware products, either onboard or offboard the weapon system, and is often purchased from lower tier subcontractors. While we did not specifically ask for information on foreign suppliers responsible for embedded software, officials for two of the programs reviewed stated that this software tends to include more reused and COTS software. These officials indicated that this could limit the visibility of the software suppliers because acceptance testing was usually only performed to prove functionality and the software was not

further evaluated to determine the actual source that developed the software code. Further, DOD and prime contractor officials told us that it is sometimes difficult to determine whether the actual hardware subcontractor developed embedded software, or if it was done by a software developer hired by that subcontractor, thus further reducing visibility of software suppliers.

While most of the program offices we reviewed did not specifically track foreign software suppliers for security purposes, almost all of the programs had opportunities to gain such knowledge through practices designed to collect other information. One way program offices obtained information on software suppliers was through requirements in their prime contracts. Many of the program offices in our review were able to obtain some information on software suppliers, either directly or indirectly, because it was contractually required. In some cases, this information was available early in the proposal process when bidders were required to identify suppliers they intended to use in the development and manufacturing phases, including potential foreign suppliers and components they were expected to provide. For example, officials from one program office said they were effective in determining software suppliers at the prime and subcontractor levels because they were intimately involved with source selection and contract negotiation. However, only five of the prime contractors reported that they were required to notify the program office concerning their decisions on software subcontracting. Once a winning bidder is selected, more information is often available to the program manager. For example, contracts for 12 programs contained a requirement that the contractors provide a software development plan that included information on some of their planned suppliers, development risks, and action plans for the contract period. In at least two cases, program software managers became aware of foreign software suppliers while collecting information requested for this review.

Program officials also said that some knowledge of foreign software development was available as a result of procedures in place because their programs contained classified or technical program information. For example, of the six programs that had significant knowledge of foreign software suppliers, four reported they had very few foreign suppliers because handling restrictions for classified information precluded the involvement of such suppliers, not because they were specifically managing software development risks. Similarly, contractors for 12 programs had information available from the export license process. While limited information on the supplier and location of foreign entities

performing software work was available from export licenses, contractors request approval directly from the State Department, which may not refer the application to DOD or the individual program offices. Consequently, program managers likely did not have this information available for use in software risk management decisions.

Program Risk Mitigation Efforts Are Focused on Meeting Performance Requirements and Are Often Delegated to Contractors

The relative importance of software security in risk mitigation efforts also varied greatly across the systems we reviewed. For 11 of the 16 systems, program managers have not identified foreign supplier involvement in software development as a significant risk to the security of their weapon systems. Instead, program managers concerned with completing their programs on budget and on schedule generally focused risk mitigation efforts on program level risks associated with the performance of system components, not on internal software development security risks. When specifically identified, software risks are usually defined by their impact when integrated with these system level risks and do not specifically focus on foreign suppliers used in software development. Software generally only becomes a concern for program managers as it begins to affect the cost or schedule of the program. For example, one of the programs we reviewed lists "software executibility" as a program level risk. The risk is based on potential cost and schedule overruns should the software not function as needed to allow related system components to meet mission requirements, rather than potential vulnerabilities from foreign suppliers. For these programs, security risks have generally been implemented to prevent unauthorized access to classified or technical program information, provide security at contractor facilities, and limit access to export-controlled technical information in accordance with ITAR license requirements, rather than specifically for software security. In addition, 12 of the programs used the Technology Assessment/Control Plan and the Program Protection Plan to ensure that risks associated with foreign participation on the program were addressed.

Programs that identified software security as a risk focused on limiting foreign access to software development facilities and denying foreign access to software code. In addition, these programs employed various measures to address software security consistent with information assurance requirements. These measures included the use of password protection, firewalls, or encrypted software, but they did not always focus on risks from foreign involvement in software development. Further, 11 programs mentioned using DITSCAP as a means for addressing general software security. However, interpretation and implementation of this requirement can vary across programs. For example, according to officials

from two programs, the current DITSCAP requirements do not govern contractors in cases where the requirements were not included as part of the original contract. Representatives from two of the programs we reviewed noted that guidance for implementing DITSCAP was confusing and that they were uncertain whether the process applied to their programs. Program officials responsible for software development on one other program indicated that they had no knowledge of this process. In cases where DITSCAP is being implemented, the certification and accreditation process requirements are determined based on the program manager's assessment of risks. If the program manager has not identified foreign software development as a program risk or threat, it will not be addressed by the process.

Because security and software risks are generally defined in terms of programmatic elements, program managers often delegate the identification and mitigation responsibility to the contractors who are developing the system and are therefore more knowledgeable about what functions are needed from the software. Officials from eight of the programs we reviewed said they expect contractors to ensure quality and security on their systems because their software development processes are more mature than those required by DOD, and that such practices could indirectly address foreign software risks. For example, contractors for these eight programs were presumed to be addressing software security because they were employing practices such as peer review [14] and software testing consistent with SEI development models.[15] Peer review is recognized as a best practice for improving software development and is generally performed to improve the quality and functionality of software

[14]Peer reviews and inspections of software, documentation, and hardware are used extensively during the requirements, design, and coding phases to identify any integration problems that must be corrected.

[15] The Software Engineering Institute has identified specific processes and practices that have proven successful in fostering quality software development. The Capability Maturity Model for Software® (registered in the U.S. Patent and Trademark Office by Carnegie Mellon University), for example, focuses on improving software development processes. The model rates software maturity according to five levels of maturity: (1) Initial: The software process is characterized as ad hoc. Success depends on individual effort; (2) Repeatable: The basic process is in place to track cost, schedule, and functionality. Some aspects of the process can be applied to projects with similar applications; (3) Defined: There is a standardized software process for the organization. All projects use some approved version of this process to develop and maintain software; (4) Managed: The organization uses and collects detailed data to manage and evaluate progress and quality; (5) Optimizing: Quantitative feedback about performance and innovative ideas and technologies contribute to continuous process improvement.

code. In terms of security, peer review can reduce the likelihood that an individual programmer can insert malicious or other harmful code. Through dedicated software testing, teams assess the quality of the software to uncover gaps and make it as defect-free as possible. However, on eight of the programs we reviewed, decisions on the amount of software code to test were made based upon the risks and benefits to the functionality of the system to be tested, not on the benefits to security. DOD and SEI officials said that the amount of effort needed to comprehensively test every line of code to ensure complete security could be physically impossible and would require immense resources.

Because contractors for the weapon systems we reviewed had not received specific direction from program managers to address risks from foreign suppliers in software development, they tended to focus on development efforts aimed at meeting stated requirements, such as software quality and functionality. In fact, officials from the 15 contractors that responded to our review indicated this was the focus of their software development activities. While SEI representatives told us that rigorous software development could help improve the quality and functionality of software by decreasing the number of errors in software code, they also said that alone their models should never be expected to completely address software security risks. Officials from one contractor we interviewed that employs practices consistent with SEI's highest level indicated that unless software security is a specific contract requirement, they would not modify their practices to address associated risks. SEI experts confirmed that the models they have developed do not include a security element and are not intended to certify that improved processes will address risks related to software security. In fact, it is possible that using software development practices to increase efficiency could lead to an increase in security vulnerability by encouraging the use of legacy and COTS software, unless risks are managed appropriately.

For several programs we reviewed, contractors made risk identification and mitigation decisions for business reasons and to avoid additional resource burdens (i.e., cost and access) associated with incorporating foreign suppliers necessary for software development, as opposed to being done for security reasons. For example, prime contractors for two programs did not use foreign subcontractors for economic reasons; namely the company wanted to maintain the software expertise within the company. While restricting foreign access solely for economic reasons could result in a decrease in software development security risks, it might also preclude foreign suppliers that could offer new capability or lower costs to the government. For example, contractor officials for three

weapon systems told us that they restrict foreign involvement in software development because it costs too much to develop and monitor security procedures to separate foreign nationals from classified and sensitive information, not because they feel their involvement is a risk to the program. In yet another case, the contractor did not want to create dedicated partitions, such as firewalls, required to prevent employees from a foreign subcontractor from accessing unauthorized information in the system design database and instead contracted with a domestic supplier. Finally, software managers for one program told us that when foreign nationals modify or update software they had developed, it was necessary to isolate test facilities to meet security requirements, which resulted in increased cost and delays to other test activities. The officials said that, in similar cases, contracting decisions might sometimes be made in favor of U.S. suppliers to avoid costs and delays.

Conclusions

Because software is increasingly responsible for advances in weapon system capabilities, it is essential that DOD and program managers take appropriate steps to identify and manage software-related risks. While DOD has made improvements to system engineering and software development practices that can reduce the likelihood of defects in software code, current methods of testing focus on the quality of software and related functionality and failures, which will not necessarily uncover malicious intent. As the amount of software on weapon systems increases, it becomes more difficult and costly to test every line of code. Further, DOD cannot afford to monitor all worldwide software development facilities or provide clearances for all potential software developers, especially for COTS software. Given the global nature of the software industry, which offers benefits to software cost and functionality needed by weapon systems, DOD also cannot afford to exclude all foreign suppliers from its programs. While program managers should be allowed discretion in managing their acquisitions, they are responsible for knowing more about who is developing software and where and for working with DOD's software assurance resources, and other organizations as necessary, so that risks can be identified and assessed accordingly. Unless this is done early in the software acquisition process, it cannot be included as part of software source selection and risk mitigation decisions and could result in increased cost and less effective security measures if risks have to be addressed later in the acquisition process.

Recommendations for Executive Action

We have previously made recommendations to DOD to adopt more effective software development practices and to increase oversight of software intensive systems to improve acquisition outcomes. While DOD attempts to better its software acquisition policies and implement new initiatives, it must take steps to ensure that security is an integral element in decision making and that program managers mitigate risks accordingly. We recommend that the Secretary of Defense take the following three actions to address risks attributable to software vulnerabilities and threats:

- Require program managers, working with software assurance experts, acquisition personnel, and other organizations as necessary, to specifically define software security requirements, including those for identifying and managing software suppliers. These requirements should then be communicated as part of the prime development contract, to be used as part of the criteria to select software suppliers.

- Based on defined software security requirements, require program managers to collect and maintain information on software suppliers, including software from foreign suppliers. This information should be evaluated periodically to assess changes in the status of suppliers and adjustments to program security requirements.

- Require the Office of the Assistant Secretary of Defense for Networks and Information Integration and the Office of the Undersecretary of Defense for Acquisition Technology and Logistics, as part of their role to review, oversee, and formulate security and acquisition practices, to work with other organizations as necessary to ensure that weapon program risk assessments include specific attention to software development risks and threats, including those from foreign suppliers. For example, certification and accreditation processes, such as DITSCAP, should include verification that software development practices contain adequate security measures to address identified risks and threats.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with our findings that malicious code is a threat that is not adequately addressed in current acquisition policies and security procedures and stated that the department is working to strengthen software related risk management activities. DOD also noted the need to enhance its risk management processes to factor in vulnerabilities analysis of proposed software products, security risks of suppliers' processes, and counterintelligence

threat information. DOD partially concurred with our three recommendations based on the concern that they place too much responsibility for risk mitigation on program managers. Although the draft report recognized that software assurance experts from the Office of the Assistant Secretary of Defense for Networks and Information Integration were necessary to support program managers in risk mitigation efforts, we broadened two of our recommendations to include acquisition and other organizations to address this concern. DOD also provided separate technical comments that we incorporated into the report as appropriate. DOD's letter is reprinted in appendix II.

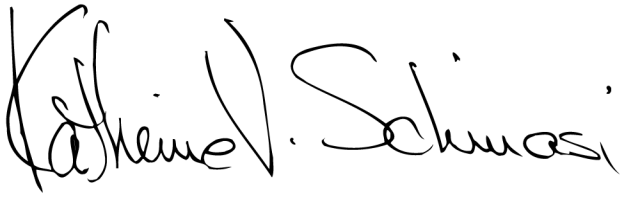
DOD agreed that software security risks should be defined for DOD weapon programs, but noted that program managers should not be solely responsible for defining security requirements, including those for identifying and managing software suppliers. Instead, DOD stated that program managers should be able to rely on external resources to gain threat information on suppliers and that formulation and oversight of security practices should be a collaborative function among several offices within DOD. While we continue to believe that program managers and software assurance experts play a critical role in defining software security requirements, we do see the value of involving other DOD resources to provide coordinated evaluation of broader security concerns. As such, we modified our recommendation to reflect the inclusion of acquisition personnel and other organizations as necessary.

DOD also agreed that information on software suppliers, including foreign suppliers, should be collected and that this information should be periodically assessed to determine if adjustments to security requirements are needed. However, DOD indicated that centralized information on software suppliers is necessary because the cost of collecting and maintaining this information would require resources and assets beyond those of individual program managers. DOD indicated its intent to develop a database to identify, track, and maintain information on security risks from specific software suppliers, which could be used by program managers across various weapon and other programs for developing acquisition strategies, plans, requests for proposals, and contracts. While we agree that such a database would be helpful to program managers in collecting and maintaining information on software suppliers, we made no change to the recommendation because the program managers should be responsible for collecting this information until such a database is developed and for directing the collection of information from the database once it is completed.

Finally, DOD agreed that it should ensure that program risk assessments include specific attention to software development risks, including those from foreign suppliers. However, DOD suggested that this might be best accomplished through collaboration between the Office of the Assistant Secretary of Defense for Networks and Information Integration, the Office of the Undersecretary of Defense for Acquisition Technology and Logistics, and the Office of the Undersecretary of Defense for Intelligence. This seemed reasonable, and we adjusted our recommendation to reflect the inclusion of other organizations. Further, DOD agreed certification activities such as DITSCAP can assist in addressing insider threats in software development, but that additional guidance is necessary to ensure that software security risks are addressed during system design and development or when selecting software sources.

We are sending copies of this report to interested congressional committees; the Secretary of Defense; the Secretaries of the Air Force, Army, and Navy; the Commandant of the Marine Corps; and the Director, Office of Management and Budget. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512- 4841. Staff acknowledgments are listed in appendix III.



Katherine V. Schinasi
Managing Director
Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To determine how the Department of Defense (DOD) measures the extent of foreign involvement in software development in weapon systems and how risks associated with using foreign suppliers for software development are measured and mitigated, we reviewed relevant DOD guidance, policies, regulations, and procedures. In addition, we spoke with DOD officials from the Office of the Under Secretary of Defense (Acquisition Technology & Logistics), the National Security Agency, the Defense Information Systems Agency, the Defense Advanced Research Projects Agency, the Office of the Assistant Secretary of Defense (Networks and Information Integration), the Department of the Army, the Department of the Air Force, and the Department of the Navy. We met with software experts at the Software Engineering Institute of Carnegie Mellon University to obtain information on software development practices and risk identification and mitigation techniques used by the software industry. Additionally, we met with the Association of Old Crows (The Electronic Warfare and Information Operations Association) whose membership includes individuals and companies involved in the design and development of software used in DOD weapon programs.

To document and analyze how programs specifically measure and manage their use of foreign-developed software, we identified 16 DOD weapon systems and solicited information from each program office and prime contractor. We selected these weapon systems based on recommendations from DOD officials and on our internal knowledge of the systems. While our selection of programs cannot be generalized to the population of all DOD systems, the systems selected varied by product type, represented each of the military services, and represented a range of DOD contractors. The systems reviewed were the Abrams System Enhancement Package, AH-64D Apache, Bradley Upgrade, C-130 Avionics Modernization Program, C-130 J Hercules, C-17 Globe Master, Comanche Reconnaissance Attack Helicopter (RAH-66), F/A-18 Super Hornet, F/A-22 Raptor, Future Combat Systems, Global Hawk Unmanned Aerial Vehicle, Joint Helmet Mounted Cueing System, Joint Strike Fighter, Patriot Missile System, Tactical Tomahawk Missile, and Wideband Gapfiller Satellites.

Using their respective command liaisons to initially contact each office, we distributed a structured set of questions to solicit information from software managers designated by individual program managers to respond to our inquiry. To further determine how programs manage and mitigate their use of foreign-developed software, we then tailored follow-up questions to solicit information and documentation in areas such as program risk identification and management practices, security policies and procedures, and software contracting management practices. To learn

more about program practices for managing and mitigating the use of foreign-developed software, we solicited information and documentation from the prime contractor for each system using contacts provided by program office officials. Information requested from contractors included government guidance for software practices, company software development and security practices, software risk mitigation efforts, software testing procedures, and software sourcing decision processes. We received information from 15 of the prime contractors through written responses, on-site interviews, and other means such as telephone conversations. We also obtained several security and software related documents such as the Program Protection Plan, the Software Development Plan, and other program specific documents, such as the contract, for the systems we reviewed.

Appendix II: Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION INTEGRATION

May 17, 2004

Ms. Katherine V. Schinasi
Director, Acquisition and Sourcing Management
U.S. General Accounting Office
Washington, D.C. 20548

Dear Ms. Schinasi,

This is the Department of Defense (DoD) response to the GAO draft report, "DEFENSE ACQUISITIONS: Knowledge of Software Suppliers Needed to Manage Risks," dated May, 2004, (GAO Code 120221/GAO-04-678). We have reviewed the report and appreciate the findings on the risks of malicious code in weapons systems software acquisition activities, particularly from foreign suppliers. We note that risks attributable to software vulnerabilities are not limited to foreign suppliers.

We agree in principle with the findings that malicious code is a threat not adequately addressed in current acquisition policy and software security procedures; however, we disagree with the recommendations as stated relative to organizational roles. Individual program managers should be able to rely on external expert resources to gain threat information on suppliers. As such, formulation and oversight of security practices will continue to be a collaborative function among several offices within the DoD best suited to meet the threat analysis needs of DoD programs.

The DoD continues to strengthen risk management activities to better focus on mitigating risks attributable to software through software acquisition process improvement programs, software assurance initiatives, and systems engineering initiatives. DoD has identified mechanisms to enhance our acquisition risk management processes to factor in vulnerability analysis of proposed products, security risks of suppliers' processes, and counterintelligence threat information. For critical assets requiring high assurance, this entails more comprehensive product diagnostic capabilities to discover malicious code and vulnerabilities, process capability evaluations of suppliers using security criteria within the framework of process standards or capability maturity models, and counter-intelligence threat assessments of prospective suppliers.
DoD will continue to strengthen threat analysis activities and security practices within

our acquisition process, including source selection, contract process monitoring, and certification activities similar to DITSCAP, to address insider threats related to the software development environment. Managing risks associated with such threats should be reviewed as part of program oversight activities.

Detailed comments to the recommendations are provided at TAB A. Technical comments have been forwarded to your staff to correct and clarify information in selected sections of the report.

The DoD Point of Contact for this action is Mr. Stanley J. Jarzombek, 703-602-1489, ext 154.

Robert G. Gorrie
Director, DIAP

Enclosure:
As stated

GAO DRAFT REPORT - MAY, 2004
GAO CODE 120221/GAO-04-678

"DEFENSE ACQUISITIONS:
KNOWLEDGE OF SOFTWARE SUPPLIERS NEEDED TO MANAGE RISKS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE RECOMMENDATIONS

GENERAL COMMENT

The DoD agrees with the report findings that malicious code is a threat, and that it is not adequately addressed in current acquisition policies and software security procedures. However, we disagree with the recommendations' suggestions regarding what organizations are best suited to address these issues. The formulation and oversight of security practices will continue to be a collaborative function among several offices within the DoD. Individual program managers should be able to rely on external resources to gain threat information on suppliers. They should not be expected to individually provide threat assessment resources or expertise on threats posed by foreign suppliers.

The DoD continues to strengthen risk management to better focus on mitigating risks attributable to software through software acquisition process improvement programs, software assurance initiatives, and systems engineering initiatives. DoD has identified mechanisms to enhance our acquisition risk management processes factoring in vulnerability analysis of proposed products, security risks of suppliers' processes, and counterintelligence threat information. For critical assets requiring high assurance, the enhanced risk management process should include counterintelligence threat assessments of prospective suppliers, more comprehensive product diagnostic capabilities to discover malicious code and vulnerabilities, and process capability evaluations of suppliers using security criteria within the framework of process standards or capability maturity models. DoD will continue to strengthen threat analysis activities and security practices within our acquisition process, including source selection, contract process monitoring, and certification activities similar to DITSCAP, to address insider threats related to the software development environment. We believe the management of risk associated with such threats should be reviewed as part of program oversight activities.

The DoD recognizes that these software risks are applicable to more than just weapons systems, and the risks must be mitigated throughout the lifecycle. We believe that the intent of all three recommendations within the GAO report could be addressed by enhancing our acquisition risk management processes. We are seeking to improve our current threat analysis processes to include threats relevant to the acquisition, development and use of software components.

Threat analysis drives the development of security requirements, and it should be carried out at the subsystem, system, and system of system levels, and not be limited to the scope, expertise and resources of individual program managers. It is only at the broadest levels that the threat context (including network connectivity) can fully be appreciated. By improving threat analysis,

and blending it into an enhanced acquisition risk management process, DoD will provide the requisite oversight and traceability. We also believe that there are limits to the availability of developer identification information at the lowest level of software components, especially in commercial and open source environments, and that risk analysis should determine when the threat is sufficiently high to warrant traceability at those levels.

Risks attributable to malicious code are applicable to other federal agencies. We believe there should be increased cooperation and support for gathering this type of information between intelligence organizations and acquisition organizations.

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense require program managers, working with DOD's software assurance experts, to specifically define software security requirements, including those for identifying and managing software suppliers. These requirements should then be communicated as part of the prime development contract, to be used as part of the criteria to select software suppliers. (p. 19/GAO Draft Report)

DOD RESPONSE 1: Partially concur. Due to resource constraints, this could not be done for all systems at present. By identifying assets that require high assurance, DoD intends to require specified programs, or categories of programs, to employ the use of enhanced acquisition risk management practices to factor in counterintelligence threat information on suppliers, vulnerability analysis of proposed products, and security risks of suppliers' processes. This would require that program managers specifically define software security requirements, including those for identifying and managing software suppliers. These requirements would then be communicated as part of the prime development contract, to be used as part of the criteria to select software suppliers. The Office of the Under Secretary of Defense (Acquisition, Technology, and Logistics) and the Office of the Assistant Secretary of Defense (Networks and Information Integration) will jointly lead the effort, in conjunction with other DoD organizations, to define generic "software security requirements" and criteria by which to judge risks associated with foreign software suppliers. As pointed out in the GAO report, software is a global industry where program managers have little or no insight into security risks associated with foreign suppliers. Domestic suppliers often depend on foreign sources for products and development. Individuals within the DoD need to work with appropriate intelligence agencies to bound the security risk problem and provide requisite policy and guidance to DoD acquisition communities. DoD will identify security risks associated with software from foreign suppliers and develop recommended security requirements for solicitation and acquisition security guides. Program managers would be expected to include guidance in acquisition programs once security requirements and criteria are defined and approved by OSD. We believe the management of risk associated with such threats should be reviewed as part of program oversight activities.

RECOMMENDATION 2: The GAO recommended that the Secretary of Defense, based on defined software security requirements, require program managers to collect and maintain information on software suppliers, including software from foreign suppliers. This information should be evaluated periodically to assess changes in the status of suppliers and adjustments to program security requirements. (p. 19/GAO Draft Report)

DOD RESPONSE 2: Partially concur. The DoD, not necessarily individual program managers, will collect and maintain information on software suppliers, including software from foreign suppliers. Identifying, tracking and maintaining intelligence on security risks of software suppliers is best done at the DoD level. DoD is seeking ways to enhance its risk management processes to factor in counterintelligence threat information, vulnerabilities analyses of proposed products, and security risks of suppliers' processes. For those critical assets that require high assurance, this would include more comprehensive product diagnostic capabilities than are presently available (to discover malicious code and vulnerabilities), process capability evaluations of suppliers using security criteria, and counterintelligence threat assessments of prospective suppliers. The evaluations and threat assessment would be requested by the program and most likely independently conducted by other organizations. Based on defined software security requirements, program managers would be required to direct the collection of information on software suppliers, including software from foreign suppliers. This information would be evaluated periodically to assess changes in the status of suppliers and adjustments to program security requirements. Collecting and maintaining information on software suppliers, including software from foreign suppliers, will require resources and assets beyond those of individual program managers. Program managers should use software security risk information on domestic and foreign software suppliers in acquisition strategies, plans, requests for proposal (RFPs), and contracts. . Services and agencies developing software should have access to a suppliers' risk database that is under the purview of an organization providing support to DoD acquisition programs.

RECOMMENDATION 3: The GAO recommended that the Secretary of Defense require the Office of the Assistant Secretary of Defense for Networks and Information Integration, as part of its role to review, oversee, and formulate security practices, to ensure that weapons program risk assessments include specific attention to software development risks, including those from foreign suppliers. For example, certification and accreditation processes, such as the DITSCAP, should include verification that software development practices contain adequate security measures to address identified risks. (p. 19/GAO Draft Report)

DOD RESPONSE 3: Partially concur. This will require collateral responsibilities between OUSD(AT&L) and OASD(NII) with participation by OUSD(Intelligence). As part of their established roles and responsibilities, to review, oversee, and formulate security practices, OUSD(AT&L) and OASD(NII) will ensure that program risk assessments include specific attention to software development risks, including those from foreign suppliers, in their program solicitations and suppliers' capability evaluations using security criteria. Evaluation and certification processes, such as the DITSCAP, do not provide appropriate guidance for system design and development, or selection of sources. Part of the needed guidance must address software security risks and risk management. Program managers have the responsibility to address software supplier security risks within their program risk management plans.

Appendix III: Staff Acknowledgments

Acknowledgments

John Neumann, Brian Mullins, Delores Cohen, Shelby S. Oakley, Christopher Miller, Gary Middleton, and Marie Ahearn made key contributions to this report.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548